Abstract

An encryption device and method and decryption device and method which implement a bit-based encryption scheme and hardware design. The encryption device includes a random number generator, receiving a main key, determining a working key using at least one random number and outputting a working key, a model, receiving the main key, the working key and plain text to be encoded and generating at least two frequency counts. The encryption device further includes an encoder, which outputs encoded text based on the working key, the plain text and the at least two frequency counts. The encryption device and method and decryption device and method progress encrypted text that is based upon a stream structure with an unlimited key length and may be compressed by 50%. The encoded text is changeable with different environments even for the same plain text and the same key. Operations of the hardware design are based on arithmetic additions and shifts, and not multiplications and divisions. As a result, the hardware design is simple and applicable to cryptography and e-commerce.